# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-307393
(43)Date of publication of application : 22.11.1996

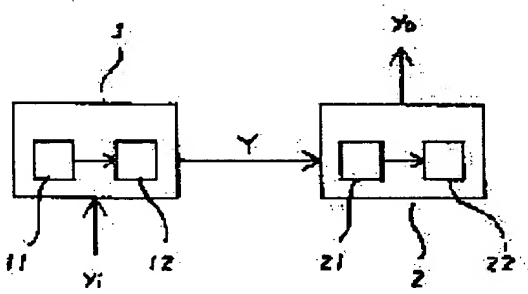
(51)Int.Cl. H04K 1/00
G09C 1/00
H04B 14/04

(21)Application number : 07-145078
(22)Date of filing : 08.05.1995

(71)Applicant : NEO TECHNOL:KK
(72)Inventor : SHONO KATSUFUSA
TAKAKUBO OSAMU

## (54) INFORMATION COMMUNICATION METHOD AND DEVICE

(57)Abstract:
PURPOSE: To attain information communication capable of executing quick processing and having high reliability by executing encoding processing by the use of branching of chaos and executing decoding processing by the use of a predictable range out of discrete time mn which the divergence and convergence of chaos are repeated.
CONSTITUTION: A digital input signal (yi) is supplied to an input part of an information communication equipment 1. The equipment 1 is provided with a chaos generation circuit 11 and a data base 12 is connected to the circuit 11. Another information communication equipment 1 is connected to an output part in the equipment 1 through a communication network and an encoded output signal Y is supplied to the equipment 2. The equipment 2 to which the signal Y is supplied is also provided with a chaos generation circuit 21 and a data base 22 is connected to the output side of the circuit 21. A decoded output signal (yo) is supplied from the output part of the equipment 2 to a communication terminal.




LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平8－307393

(43)公開日　平成８年(1996)11月22日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｈ０４Ｋ　1/00 | | | Ｈ０４Ｋ　1/00 | Ｚ | |
| Ｇ０９Ｃ　1/00 | | 7259－5Ｊ | Ｇ０９Ｃ　1/00 | | |
| Ｈ０４Ｂ　14/04 | | | Ｈ０４Ｂ　14/04 | Ｚ | |

審査請求　未請求　請求項の数９　書面　（全 6 頁）

(21)出願番号　特願平7－145078

(22)出願日　平成７年(1995)５月８日

特許法第30条第１項適用申請有り　1995年３月10日　社団法人電子情報通信学会発行の「1995年電子情報通信学会総合大会講演論文集　基礎・境界」に発表

(71)出願人　593175235
株式会社ネオテクノロジー
東京都千代田区神田小川町２丁目12番　信愛ビル

(72)発明者　庄野　克房
神奈川県横浜市旭区白根町５丁目45番12号

(72)発明者　高窪　統
東京都世田谷区祖師谷６丁目17番７号

(54)【発明の名称】　情報通信方法および装置

(57)【要約】
【目的】　汎用情報機器や通信ネットワークにおいて、カオスの有する分岐と発散、収束を用いて符号化や復号を可能にする。
【構成】　電子回路で発生するカオスの分岐を用いて信号を符号化し、カオスの発散と収束を繰り返す離散時間列のうち予測可能な範囲を用いて符号化された信号を復号する。

1

【特許請求の範囲】

【請求項1】カオスの分岐を用いて信号を符号化する符号化処理を行い、カオスの発散と収束を繰り返す離散時間列のうち予測可能な範囲を用いて前記符号化された信号を復号する復号処理を行うことを特徴とする情報通信方法。

【請求項2】前記符号化処理および／または復号処理を、離散時間tに関するカオスの内部状態y（t）をAD変換してデジタルコードY（t）に変換し、データベースに蓄える該デジタルコードY（t）に基づいて行うことを特徴とする請求項1記載の情報通信方法。

【請求項3】前記データベースには、離散時間tに関するカオスの前記デジタルコードY（t）として過去の状態に対応するデジタルコードY（t－τ）を蓄え、該データベースに基づいて信号の符号化処理を行うことを特徴とする請求項2記載の情報通信方法。

【請求項4】前記データベースには、離散時間tに関するカオスの前記デジタルコードY（t）として過去から現在にもどした状態に対応するデジタルコードY（t－τ＋τ）を蓄え、該データベースに基づいて符号化された信号の復号処理を行うことを特徴とする請求項2記載の情報通信方法。

【請求項5】信号をカオスの分岐を用いて符号化した符号化信号を出力するカオス回路と、該符号化信号を受信して発散と収束を繰り返す離散時間列のうち予測可能な範囲を用いて該符号化信号を復号するカオス回路を備えることを特徴とする情報通信装置。

【請求項6】離散時間tに関するカオスの内部状態y（t）をAD変換したデジタルコードY（t）のデータベースを備える請求項5記載の情報通信装置。

【請求項7】離散時間tに関するカオスのデジタルコードY（t）のデータベースがROMであることを特徴とする請求項6記載の情報通信装置。

【請求項8】離散時間tに関するカオスの前記デジタルコードY（t）のデータベースには、過去の複数の状態に対応するデジタルコードY（t－τ）を符号化コードとして蓄えることを特徴とする請求項6記載の情報通信装置。

【請求項9】離散時間tに関するカオスの前記デジタルコードY（t）のデータベースには、過去から現在にもどした状態に対応するデジタルコードY（t－τ＋τ）を復号化コードとして蓄えることを特徴とする請求項6記載の情報通信装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、電子回路で発生するカオスを用いることにより信号の符号化処理と復号処理を行う情報通信方法および装置に関し、無線によるか有線によるかを問わず、電話、ファクシミリ、コンピュータ、情報端末機器などの各種の情報機器の内部、あるいは、これらの情報機器により構築される通信ネットワークなどに用いる情報通信方法および装置に関するものである。

2

【0002】

【従来の技術】コンピュータや情報端末機器などの情報機器の内部における情報通信、あるいは、これらの情報機器により構築される通信ネットワークにおける情報通信では、デジタルシステムが広く採用されており、デジタル信号によって各種の情報が授受されている。しかるに、外交文書や金融情報、プライバシー情報など、守秘性の強い情報を授受する場合には、安全確実で信頼できる情報通信方式や情報機器の実現が不可欠である。そこで、通信の信頼性を高め、プライバシーの保護や秘密情報の漏洩防止、盗聴の防止などを図るため、信号の符号化処理や復号処理の研究が盛んに行われている。

【0003】かかる従来技術は暗号処理技術として知られており、典型的には、大型計算機を用い、暗号表あるいは乱数表と高度な計算式を駆使することにより、秘密文書を一括処理して符号化あるいは復号するものである。

【0004】

【発明が解決しようとする課題】しかしながら、上記の従来技術によれば、大型計算機による複雑な計算処理によって文書や情報を一括して符号化、あるいは、復号するので、暗号化処理や復号化処理のために長時間を要して情報授受に遅れが生じてしまう。しかも、大型計算機や複雑な計算処理用ソフトウェアなど、高価な設備等が必要になるので、一般の産業界がで汎用的に使えるものではなかった。このため、一般の情報通信にあっては、信号の符号化や復号処理を汎用的に採用することは困難であり、故に、情報通信には秘話機能などの高い信頼度を期待できず、プライバシー情報の流出や銀行バンキングシステムでのコンピュータの不正使用、あるいは、警察無線やコードレス電話の漏話や盗聴による漏洩、携帯電話での混信や混線など、様々な社会的問題が生じている。

【0005】一方、今日の高度に情報通信に依存した社会では、コンピュータや電話などの情報機器の内部において、あるいは、これらの情報機器によって構築される通信ネットワークにおいて、汎用的に使用でき、簡便な構成で、しかも、迅速に信号の符号化処理と復号処理が行える情報通信技術の実現が喫緊な課題になっている。

【0006】この発明は、電子回路で発生したカオスを用いることにより、情報機器の内部、あるいは、通信ネットワークにおいて汎用的に信号の符号化と復号ができる情報通信方式と装置を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するために、この発明の情報通信方法および装置では、電子回路で発生するカオスを用いて信号の符号化と復号を行うも

のであり、カオスのアナログ現象をＡＤ変換してデジタルコードに変換し、該デジタルコードをデータベースに蓄え、該ベータベースを利用して逐次処理により信号の符号化と復号化を行うものである。

【０００８】この発明の一の情報通信方法は、カオスの分岐を用いて信号を符号化する符号化処理を行い、カオスの発散と収束を繰り返す離散時間列のうち予測可能な範囲を用いて前記符号化された信号を復号する復号処理を行うものである。

【０００９】そして、上記情報通信方法において、前記符号化処理および／または復号処理を、離散時間ｔに関するカオスの内部状態ｙ（ｔ）をＡＤ変換してデジタルコードＹ（ｔ）に変換し、データベースに蓄える該デジタルコードＹ（ｔ）に基づいて行うことができる。

【００１０】さらに、上記情報通信方法において、前記データベースには、離散時間ｔに関するカオスの前記デジタルコードＹ（ｔ）として過去の状態に対応するデジタルコードＹ（ｔ－$\tau$）を蓄え、該データベースに基づいて信号の符号化処理を行うこともできる。

【００１１】さらにまた、上記情報通信方法において、前記データベースには、離散時間ｔに関するカオスの前記デジタルコードＹ（ｔ）としてデータベースに蓄えた過去から現在にもどした状態に対応するデジタルコードＹ（ｔ－$\tau$＋$\tau$）を蓄え、該データベースに基づいて符号化された信号の復号処理を行うことができる。

【００１２】また、この発明の情報通信装置は、信号をカオスの分岐を用いて符号化した符号化信号を出力するカオス回路と、該符号化信号を受信してカオスの発散と収束を繰り返す離散時間列のうち予測可能な範囲を用いて該符号化信号を復号するカオス回路を備えるものである。

【００１３】上記情報通信装置において、離散時間ｔに関するカオスの内部状態ｙ（ｔ）をＡＤ変換したデジタルコードＹ（ｔ）のデータベースを備えることができる。

【００１４】そして、上記情報通信装置には、離散時間ｔに関するカオスのデジタルコードＹ（ｔ）のデータベースを蓄えるＲＯＭを備えると好適である。

【００１５】さらに、上記情報通信装置において、離散時間ｔに関するカオスの前記デジタルコードＹ（ｔ）のデータベースには、過去の複数の状態に対応するデジタルコードＹ（ｔ－$\tau$）を符号化コードとして蓄えることもできる。

【００１６】また、上記情報通信装置において、離散時間ｔに関するカオスの前記デジタルコードＹ（ｔ）のデータベースには、過去から現在にもどした状態に対応するデジタルコードＹ（ｔ－$\tau$＋$\tau$）を復号化コードとして蓄えることもできる。

【００１７】

【作用】上記のように構成された情報通信方法および装置の作用について以下に説明する。なお、以下の説明では、「符号」をさらに具体的に「秘話」あるいは「暗号」として表現する場合がある。

【００１８】カオス発生回路によって発生するカオスの内部状態ｙ（ｔ）は、許される内部状態の範囲内で発散と収束、分岐を繰り返す。そして、内部状態ｙ（ｔ）をＡＤ変換してデジタルコードＹ（ｔ）に変換すると、デジタルコードＹ（ｔ）は、上記の許される内部状態の範囲に対応してデジタルレンジＲを有することになる。ここで、デジタルレンジＲはデジタルコードＹ（ｔ）の最大値Ｙｍａｘ（ｔ）と最小値Ｙｍｉｎ（ｔ’）の差で与えられる。なお、ｔおよびｔ’は、カオス発生回路の制御パルスにより刻まれる離散時間である。

【００１９】デジタルレンジＲは、符号化して扱われるべき入力信号の数ｎに応じたリターンレンジＲ１、Ｒ２、・・・、Ｒｎに分割される。なお、上記分割は、必ずしも均一に等分されるとは限らない。また、各リターンレンジＲ１、Ｒ２、・・・、Ｒｎの中心に秘話として取り扱う入力信号Ｙ１、Ｙ２、・・・、Ｙｎを割り当てるのが一般的である。

【００２０】カオスは分岐構造を有するので、カオスのＡＤ変換された現在の内部状態のデジタルコードＹｉ（ｔ）（ｉは１、２、・・・、ｎの１つ）に対して、離散時間を$\tau$だけ過去にもどったデジタルコードＹｉ（ｔ－$\tau$）は、複数個が存在する。

【００２１】上記により過去にもどった複数個のデジタルコードＹｉ（ｔ－$\tau$）は、離散時間$\tau$だけ将来にむかうとＹｉ（ｔ－$\tau$＋$\tau$）となる。その結果、１つのデジタルコードＹｉ（ｔ）に対して、離散時間$\tau$を加味すると、Ｙｉ（ｔ－$\tau$）とＹｉ（ｔ－$\tau$＋$\tau$）には、発散と収束にもとづくあいまいさの幅がともなうことになる。そして、Ｙｉ（ｔ－$\tau$＋$\tau$）が上記により割り当てられたリターンレンジＲｉの中に位置する場合には、入力信号Ｙｉ（ｔ）と秘話信号Ｙｉ（ｔ－$\tau$）、復号（以下、復元ともいう）信号Ｙｉ（ｔ－$\tau$＋$\tau$）の間に密接不可分な有意味な関係があることになる。すなわち、カオスの過去への分岐を利用することにより秘話信号を得ることができ、また、カオスの将来への決定論的性質を利用することにより復元信号を得ることができる。なお、１ビット幅の入力信号Ｙｉ（ｔ）に対してＹｉ（ｔ－$\tau$＋$\tau$）の幅がＲｉ／２以下のときには、誤りのない復元が可能になる。

【００２２】ここで、１つのデジタルコードとして入力する入力信号Ｙｉ（ｔ）に着目すれば、タイムシリーズＹ（ｔ）－ｔ上を検索することによって、デジタルコードＹｉ（ｔ）を見いだすことができる。

【００２３】上記タイムシリーズについて、図２を参照して説明すると以下の通りである。すなわち、図２は、離散時間ｔに関するカオスのデジタルコードＹ（ｔ）のタイムシリーズを示す説明図である。なお、理解の容易

のために、以下の説明では、一例としての具体的数値を用いている。図２において、横軸ｔはｔ＝０からｔ＝１００までの離散時間を示し、縦軸Ｙ（ｔ）はカオスの内部状態ｙ（ｔ）を１２ビットにＡＤ変換したデジタルコードを示している。また、Ｙ（ｔ）の最大目盛りは$2^{12}$＝４０９６とした。Ｙ（０）＝２０００を初期値としている。ここで、Ｙ（１）は、初期値Ｙ（０）＝２０００を入力とするカオス発生回路の出力である。ついで、Ｙ（２）は、Ｙ（１）を入力とするカオス発生回路の出力である。順次、この操作を繰り返すことにより、タイムシリーズＹ（ｔ）－ｔが得られる。離散時間ｔの最大値は、１２ビットＡＤ変換器の場合、標準的には$2^{15}$＝３２７６８である。

【００２４】上記によるタイムシリーズの離散時間ｔの値としては、許される内部状態のデジタルレンジＲよりも十分大きな値が選ばれる。そして、タイムシリーズ上を検索することにより、１つの入力信号Ｙｉ（ｔ）に等しい内部状態が、多数回、見いだすことができる。タイムシリーズ上で見いだされる１つの入力信号Ｙｉ（ｔ）に対するタイムシリーズ上の過去$\tau$における内部状態の値Ｙｉ（ｔ－$\tau$）は、１個である。しかし、異なる離散時間における入力信号Ｙｉ（ｔ）に対するＹｉ（ｔ－$\tau$）は、カオスの分岐構造のため、同じ値（コード）になるとは限らず、１つの入力信号Ｙｉ（ｔ）に対し複数の対応するＹｉ（ｔ－$\tau$）が存在する。したがって、Ｙｉ（ｔ－$\tau$）は予測できない秘話信号となる。

【００２５】電子回路であるカオス発生回路は、１つの入力に対して、１つの決定論的出力を持つ。過去において分岐した内部状態Ｙｉ（ｔ－$\tau$）は、その値を初期値として入力したとき、未来においては１つの内部状態Ｙｉ（ｔ－$\tau$＋$\tau$）に収束する。ただし、カオスのタイムシリーズ上の状態の遷移にあっては、リヤプノフ指数$\lambda$にもとづく発散はさけられない。そのためにリターンレンジＲｉを用意しておく必要がある。

【００２６】

【実施例】この発明のカオスを用いた信号符号化と信号復号化を行う情報通信装置の実施例を以下に説明する。

【００２７】図１は、電子回路であるカオス発生回路を有する情報通信装置の概略の構成を示すブロック図である。情報通信装置１の入力部には、図示されぬコンピュータなどの通信端末が接続され、デジタル入力信号ｙｉが供給される。情報通信装置１はカオス発生回路１１を内部に備え、カオス発生回路１１にはデータベース１２が接続されている。この情報通信装置１の出力部には、図示されぬ通信ネットワーク経由で外部の別な情報通信装置２が接続されており、情報通信装置２に符号化された出力信号Ｙが供給される。通信ネットワークを経由して伝送される上記符号化された信号Ｙが供給される別な情報通信装置２にもカオス発生回路２１が内部に備えられており、カオス発生回路２１の出力側にはデータベース２２が接続されている。そして、この情報通信装置２の出力部には図示されぬコンピュータなどの通信端末が接続され、復号化された出力信号ｙｏが通信端末に供給される。



【００２８】具体的にこの実施例を詳しく説明すれば以下の通りである。すなわち、入力信号が例えば２７種類の英文小文字と５種類の記号による入力信号であり、５ビットコードで与えられるこれらの３２種類の入力信号を用いた文書作成の場合を例として説明する。１２ビットのＡＤ変換により測定されたカオスの許される内部状態のレンジが１３１２ビットであるとする。入力コードに対するリターンレンジＲｉは４１ビットである。中心コードに１ビット幅の入力信号Ｙｉ（ｔ）が割当てられ、上下には２０ビットの広がりを持つリターンレンジＲｉ＝４１が定義される。

【００２９】文字を割り当てられたリターンレンジＲｉの中心ビットＹｉ（ｔ）を、タイムシリーズのデータベース上で検索し、デジタルコードＹｉ（ｔ）を発見したら、$\tau$だけ過去にもどり秘話通信コードＹｉ（ｔ－$\tau$）を発見する。入力された英文字は入力と同時に、タイムシリーズの検索により逐次秘話コードＹｉ（ｔ－$\tau$）に変換される。

【００３０】たとえば文字”ｆ”に対応する秘話コードＹｉ（ｔ－$\tau$）は、$\tau$＝６の場合５種類のコードに変換される。秘話コードＹｉ（ｔ－$\tau$）はカオス発生回路の非線形関数による繰り返しの写像の結果であり、５種類のコードの中でどのコードがどういうひん度で現れるかを予想することはカオスの性質上困難である。

【００３１】カオスのタイムシリーズ上で内部状態にはリヤプノフ指数$\lambda$に依存した予測可能性の領域があり、$\tau$がその可能性の範囲内であれば、正しくリターンレンジＲｉの中に復元コードＹｉ（ｔ－$\tau$＋$\tau$）が入る。リヤプノフ指数$\lambda$＝０．２５の場合、$\tau$＝６以下は予測可能な範囲内ということができる。

【００３２】入力信号は文字コードに限らない。デジタルコード化した数字列であってもよい。たとえば、６ビット単位に分割して逐次秘話化を実行する場合、レンジＲは６４に分割される。分割したリターンレンジＲｉに応じて過去にさかのぼる離散時間$\tau$が決定される。内部状態ｙ（ｔ）は、十分に長い離散時間について測定を行うと、固有の分布をもち、片寄りがあるのが普通である。分布を考慮してリターンレンジＲｉや入力信号Ｙｉ（ｔ）の割当を行うとタイムシリーズ上での検索時間を短縮できる。

【００３３】カオスの内部状態ｙ（ｔ）をＡＤ変換してえられるデジタルコードＹ（ｔ）のタイムシリーズはデジタルデータベースである。デジタルコンピュータのＤＲＡＭに一連のタイムシリーズのデータを収容してデータ処理を実行することができる。このデジタルデータベースをＲＯＭチップに書き込んだハードウエアチップと

7

して用意すると、さらに高速な処理が可能となり、データの保存性も向上する。

【００３４】なお、究極の暗号化は、ｎ＝２、たとえば、Ｒ１＝”０”、Ｒ２＝”１”の１ビット単位での暗号化と復号化である。判断回路のハード化が容易にできるという点で、スピードが要求される音声の暗号化や復号化に特に有効である。

【００３５】以上説明したように、この発明によれば、カオスの内部状態が分岐のために複雑となり、将来が決定論的に決定されることを用いてデジタル入力コードを符号化でき、カオスの予測可能性の範囲で復号化できる。従って、この発明を情報通信システムに適用すれば、簡易な構成によって逐次処理による秘話機能を実現することができ、リアルタイム（実時間）処理を必要とする音声の秘話通信にも有効である。また、文字コードを入力するワードプロセッサの逐次秘話変換を可能にし、コンピュータの中の記憶コードをすべて秘話コードにできる。総じて、高度な情報通信社会において安全確実な情報伝達を簡便な構成で実現でき、極めて社会的意義の大きいものである。また、データベースとして提供されるＲＯＭの中に、複数個のカオスのタイムシリーズをもたせることができるので、複数のユーザが固有の秘話キーをもって相互に秘話コードを書き換えながら利用する秘話機能システムが可能となる。

【００３６】

【発明の効果】この発明の情報通信方式によれば、以上説明したように、カオスの分岐を用いて符号化処理を行

8

い、カオスの発散と収束を繰り返す離散時間のうち予測可能な範囲を用いて復号処理を行うようにしたので、情報機器の内部や、情報機器により構築される通信ネットワークでの情報通信において、符号化と復号を逐次、迅速に処理でき、信頼性に優れた情報通信を実現できる。また、この発明の情報通信装置によれば、信号の符号化と復号を、カオスを発生する電子回路であるカオス発生回路により行うようにしたので、集積化や小型化が容易であり、各種の情報機器や通信ネットワークに汎用的に組み込んで使用できる簡易かつ安全確実な情報通信機器を実現できるという優れた効果を奏する。また、この発明によれば、カオスのアナログ現象をＡＤ変換して得るデジタルコードをデジタルデータベースに蓄えることができるので、符号化と復号を逐次処理する情報機器の回路部分を集積化でき、情報機器全体の構成を一段と簡素化できる。

【図面の簡単な説明】

【図１】カオス発生回路を有する情報通信装置の構成を示すブロック図である。

【図２】タイムシリーズを説明する説明図である。

【符号の説明】

１、２　情報通信装置

１１、２１　カオス発生回路

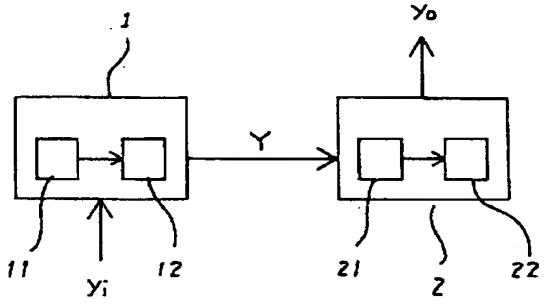
１２、２２　データベース

ｙｉ　デジタル入力信号

Ｙ　符号化された信号

ｙｏ　復号化された信号

【図１】



【図２】